

# **Transportation Worker Identification Credential (TWIC)**

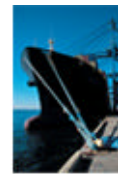
## **Stakeholder Brief**



## ***Transportation Security Administration Credentialing Program***



## ***TWIC Program***



## **Vision**

Improve security by establishing a system-wide common credential, used across all transportation modes, for all personnel requiring unescorted physical and/or logical access to secure areas of the transportation system.

## **Goals**

- Improve security
- Enhance commerce
- Protect personal privacy



## *Legislative Mandates*



### **USA PATRIOT Act of 2001**

Requires states to conduct background checks through the Attorney General and TSA before issuing licenses to individuals to transport hazardous materials in commerce.

### **Aviation and Transportation Security Act of 2001 (ATSA)**

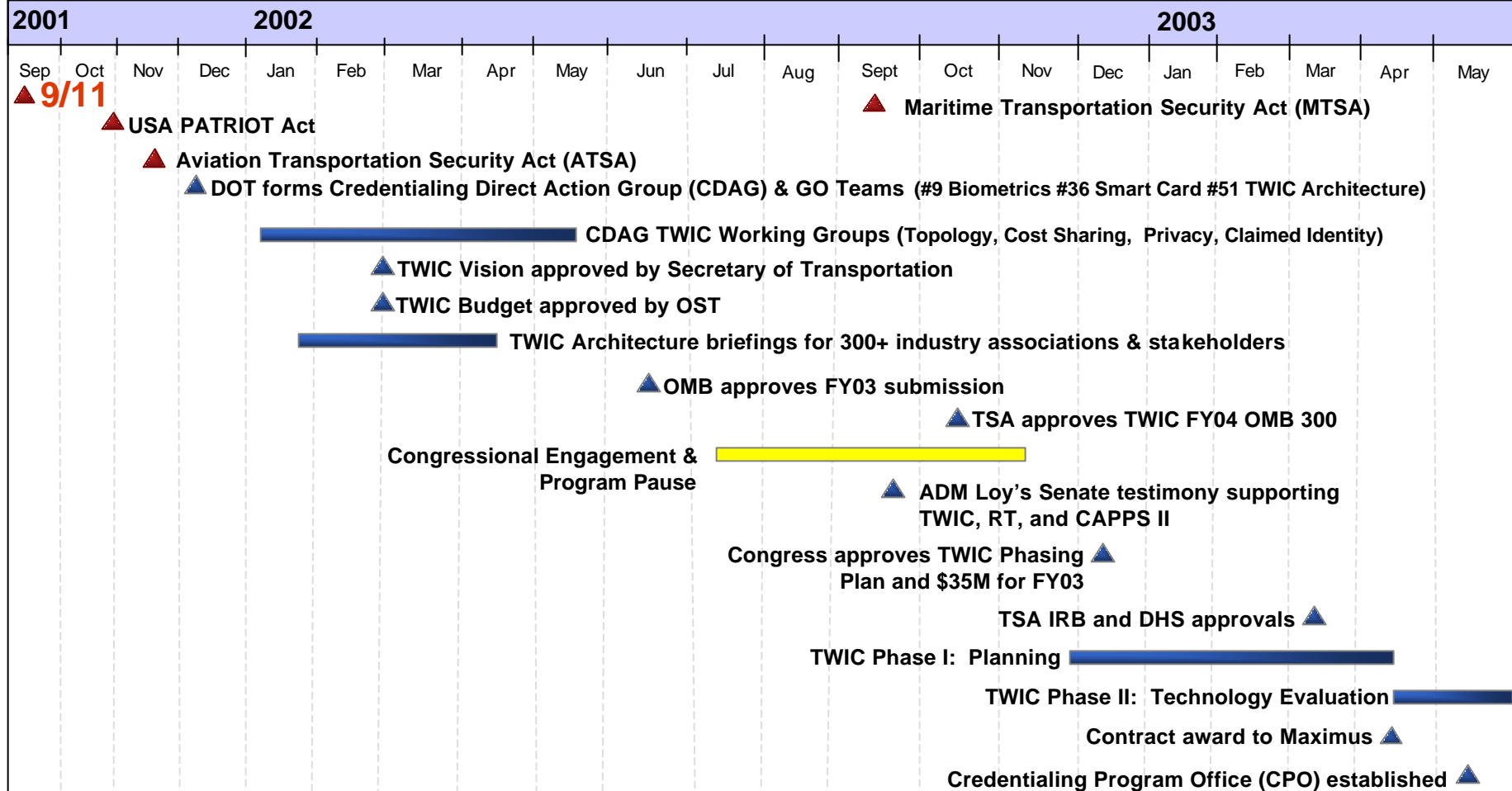
Grants TSA's Administrator broad authority for transportation security; requires TSA to ensure the adequacy of security measures at airports; directs strengthened access control points in airport secured areas; and, requires TSA to consider the use of biometric, or similar technologies, to identify individuals employed at airports.

### **Maritime Transportation Security Act of 2002 (MTSA)**

Requires the issuance of biometric transportation security cards and the completion of background checks for entry to any secured area of a vessel or facility.



# TWIC Program History



- **TWIC Legislative Authority**
  - USA PATRIOT, ATSA 2001, MTSA 2002
- **Cabinet Level (DOT) Approval Feb 2002**
- **TWIC Public Meetings Jan-Apr 2002**

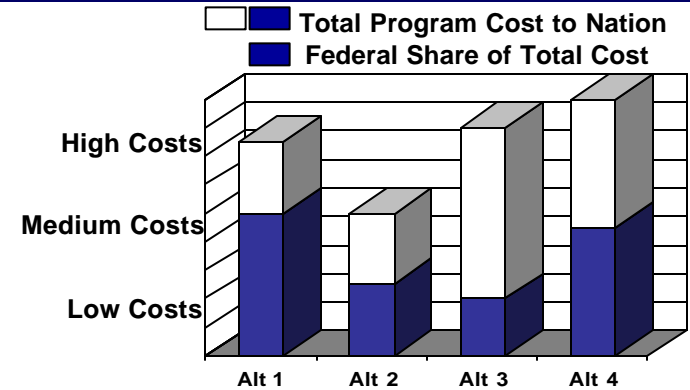
- **Congress Approved TWIC Regional Plan and \$35M for FY03**
- **President's FY04 Budget Includes \$55M for TWIC**
- **ADM Loy Strongly Supports TWIC in Testimony: "TWIC is Flagship Program"**



# Alternatives Analysis



## Conducting evaluation of Alternative 2 based on Alternatives Analysis and Balanced Scorecard results.



Alternative 1:  
Federal Implementation  
and Funding

- Common infrastructure
- Matches individual with credential technology
- Centralized control of implementation

- High system replacement costs
- Public perception / privacy concerns
- Potential impact on commerce

STOP

Alternative 2:  
Federally led Public /  
Private Partnership

- Common infrastructure
- Matches individual with credential technology
- Leverage existing systems
- Options for shared cost

- Requires local commitment to Public / Private Partnership

INVESTIGATE

Alternative 3:  
Federal Requirements /  
Local Implementation and  
Funding

- Stakeholder independence
- Matches individual with credential technology
- Local acceptance

- Divergent to interoperability goal
- Requires 100% local implementation, design, and execution
- Lack of economy of scale

STOP

Alternative 4:  
Federally led Public / Private  
Partnership with Low-Tech  
Credential

- Lower initial costs
- Common infrastructure

- Security vulnerabilities due to low technology credential
- Higher labor costs for human sensors at checkpoints

STOP



# Work Streams



Today

## Pilot Programs

### Planning (3 Months)

As-Is / To-Be  
Requirements Baseline  
Technical Evaluation Plan



### Technology Evaluation (5 Months)

Evaluate range of potential technologies for  
core business process and requirements



### Prototypes (7 Months)

Evaluate technology for full range of  
business processes, policies and  
requirements

## Business Case Development

Concept Paper  
Feasibility Study

Alternatives Assessment  
Cost Benefit Analysis

Life Cycle Cost Estimate  
Risk Management Plan

As-Is Analysis  
To-Be Analysis

## Acquisition / Procurement Tasks

Program Support  
Technical Evaluation

Pilot Evaluation

Broad Agency Announcement  
Memorandum of Agreement

## Information Technology Infrastructure and Enterprise Architecture

Regional Database  
Connectivity

Data Model  
Enterprise Information

Biometrics

Technical Architecture  
Central Database

Operations & Maintenance  
Help Desk

## Business Policy Issues

Background Checks  
Liability

Topology/Biometrics  
Cost Sharing

Privacy  
Claimed Identity

Trusted Agent  
Regulations

## Stakeholder Engagement

Workers  
Industry

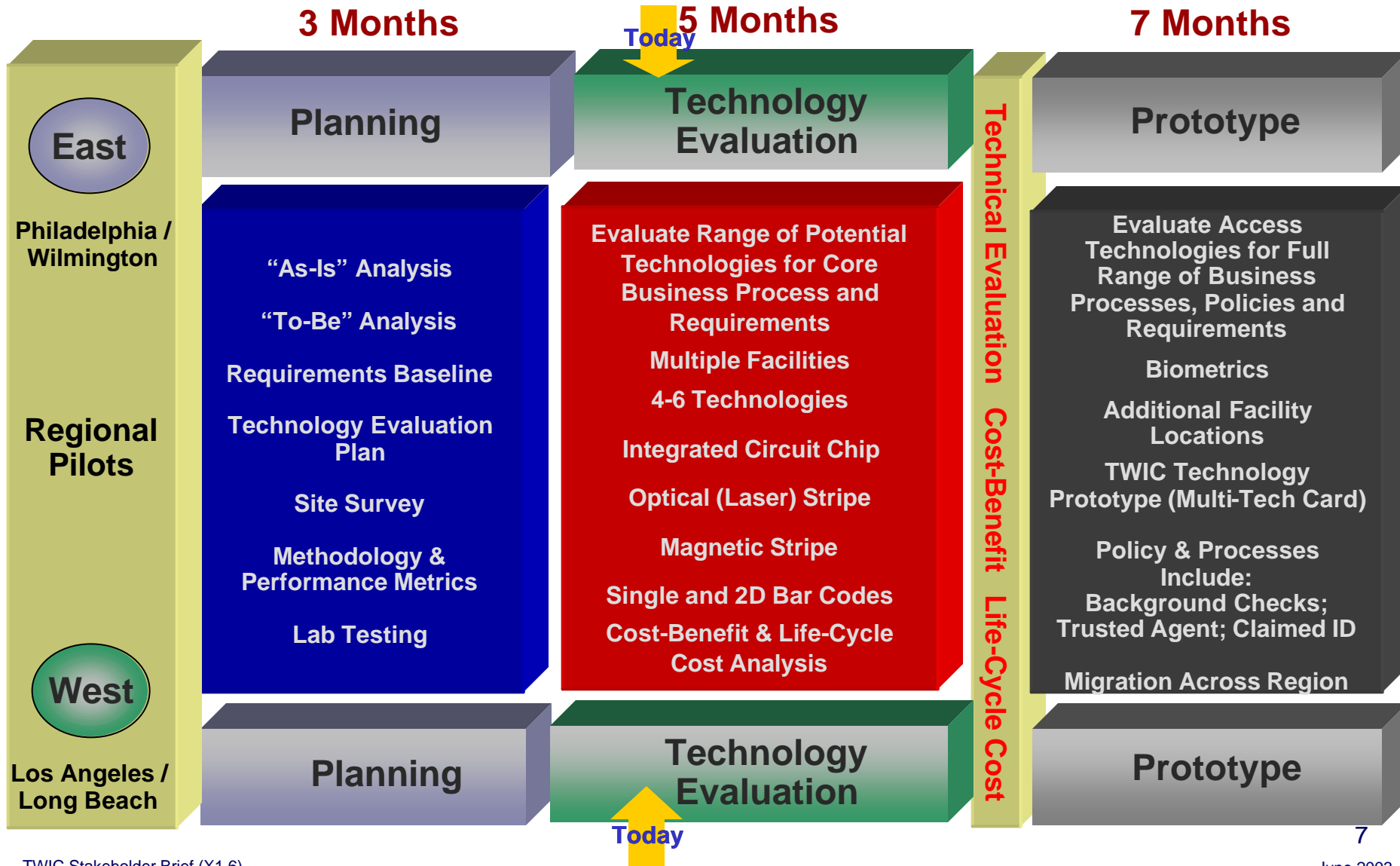
Modes  
Government

Associations  
Vendors

Local – Delaware River Region  
Local – L.A. / Long Beach



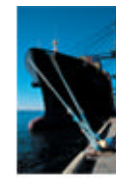
# Regional Pilots







# Technology Evaluation Details



Illustrative

Purpose  Evaluate multiple access control technologies for core business processes and requirements		Maritime							HQ			Pipeline	Air			Rail		Other		
		Port of Wilmington DE	Packer Avenue Terminal PA	Penns Terminal PA	Beckett Street Terminal NJ	APL Terminal CA	LBCT Terminal CA	Crowley Marine CA	Delaware Bay Maritime Exch PA	Port HQ Long Beach CA	Port HQ Los Angeles CA	Conoco Phillips Oil Refinery PA	PHL Airport PA	PNE Airport PA	LAX Airport CA	CSX Facility PA	Union Pacific Rail ITCF CA	Customs House PA	ILWU Union Hall CA	Salem Nuclear Plant NJ
Access Control Technologies	Enrollment	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X			
	Optical (Laser) Memory Stripe				X			X	X		X			X						
	ICC	X				X			X			X			X		X			
	Bar Code (2D)	X					X		X											
	Bar Code (3x9)		X						X							X				
	Magnetic Stripe								X	X			X		X					

## Multiple Types of Access Control Points

- Vehicle gates
- Truck multi-lanes
- Unmanned personnel turnstiles
- Building and door access
- High volume pedestrian entrances
- SIDA

## Multiple Transportation Modes

- Port, Airport, Trucking, Rail, Pipeline, and HQs

## Multiple Access Control Technologies

- Smart Chip, Magnetic Stripe, Optical Media, Single and 2D Barcodes





# Prototype Phase Details

Illustrative



Purpose		Maritime								HQ			Pipeline		Air			Rail		Other		
Broaden evaluation using multiple technologies for the full range of business processes and requirements		Port of Wilmington DE	Packer Avenue Terminal PA	Penns Terminal PA	Beckett Street Terminal NJ	APL Terminal CA	Maersk Terminal CA	LBCT Terminal CA	Crowley Marine CA	Delaware Bay Maritime Exch PA	Port HQ Long Beach CA	Port HQ Los Angeles CA	BP Refinery CA	Conoco Phillips Oil Refinery PA	PHL Airport PA	PNE Airport PA	LAX Airport CA	CSX Facility PA	Union Pacific Rail ITCF CA	Customs House PA	ILWU Union Hall CA	Salem Nuclear Plant NJ
Business Processes	TWIC Multi-Application / Multi-Technology Solution	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Contact-less	X								X	X	X			X							X
	Biometrics	X			X				X	X	X	X					X	X	X			X

## Business Processes

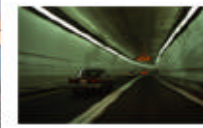
- Biometrics
- Background Checks
- Claimed Identity
- Central Database
- Watch List
- Threat Data
- Liability
- Privacy
- Trusted Agent
- Topology
- Enrollment Centers

## Analysis

- Cost-Benefit Analysis
- Life Cycle Cost Analysis
- Technical Evaluation
- Implementation Options



# TWIC System Components



## WORKER



**Card**

## FACILITY LA / Long Beach Region



Seaports  
Airports  
Pipelines

**Readers**



**Readers**

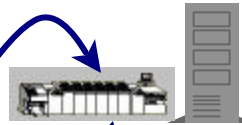


Seaports  
Airports  
Pipelines

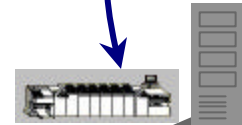


Delaware River  
Basin

## REGIONAL



Secure Network /  
Database and  
Card Production



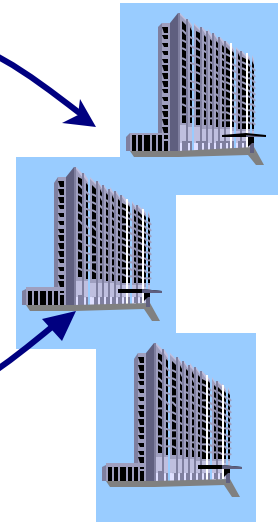
Secure Network /  
Database and  
Card Production

## CENTRAL



Central Database  
and Card  
Production

## DATA SOURCES



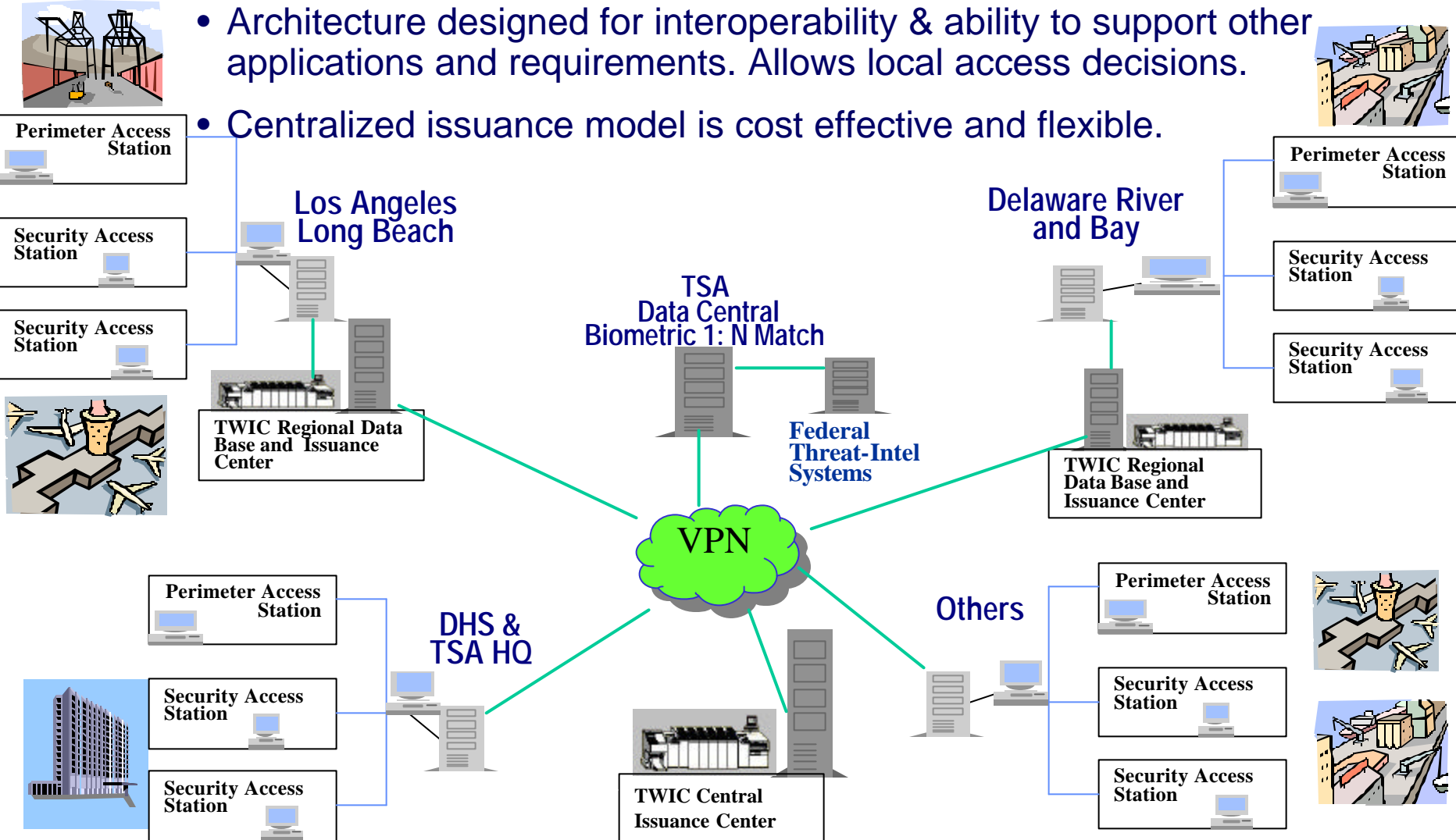
- Watch Lists
- Criminal Records
- Background Checks



# System Overview



- Architecture designed for interoperability & ability to support other applications and requirements. Allows local access decisions.
- Centralized issuance model is cost effective and flexible.





## ***TWIC System Attributes***



- Positive match of credential – person - background check - access level through the use of a secure reference biometric
- Business and standards based approach and flexible solution architecture enables TWIC System to support multiple users, requirements and applications
  - Government Smart Card Interoperability Specification (GSC-IS) provides broad interoperability
  - Open architecture and multiple technologies support leveraged investments
  - TWIC is a tool that enables business process improvements and E-Gov
  - Capable of meeting needs across DHS
- Centralized ability to interface with other federal agencies and databases for “watch list”, threat and intelligence information
- Secure record control and network of databases, provides capability to disseminate “threat alerts”, revoke security access system-wide for specific individuals, hot-list, or deal with lost-stolen cards
- Reduces risk of fraudulent / altered credentials through use of state-of-the-art anti-tamper and anti-counterfeit technologies



# Card Architecture



## Illustrative of Surface Technologies

Linear Bar Code

2D Bar Code

Magnetic Stripe

ICC Chip

Optical (Laser) Media Stripe

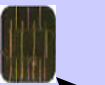
Transportation Security Administration  
TRANSPORTATION WORKER  
IDENTIFICATION CREDENTIAL  
TWIC



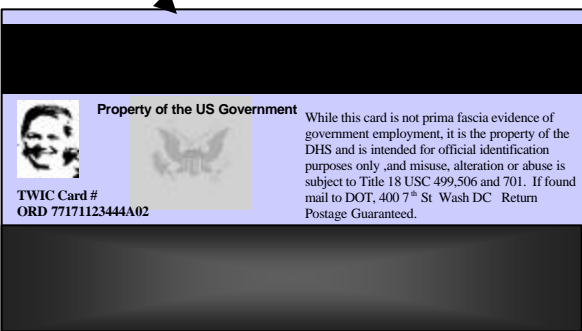
Name  
Jane Smith

Employer  
Regional Airline

Issue Date  
2002SEP19  
Expiration Date  
2003SEP20



Issue Date  
2002SEP19  
Expiration Date  
2003SEP20



ISO Standards

Interoperable via GSC-IS

FIPS 140 Level 2 Secure

JAVA 32-64K EEPROM

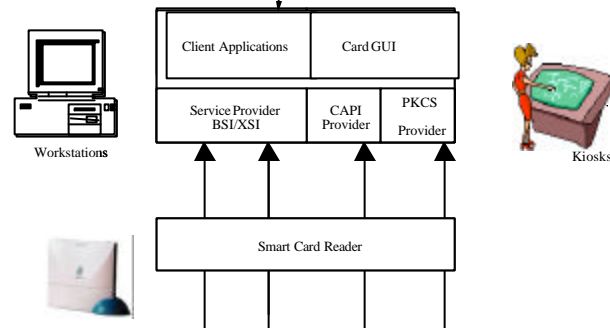
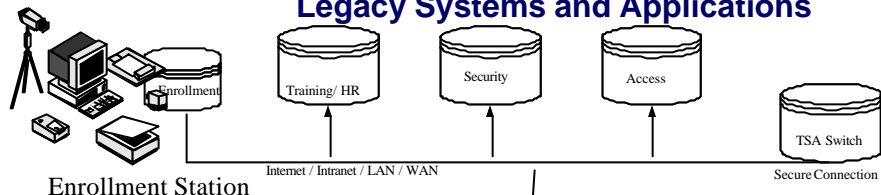
Multi-Technology Card

PKI

Multiple Biometrics

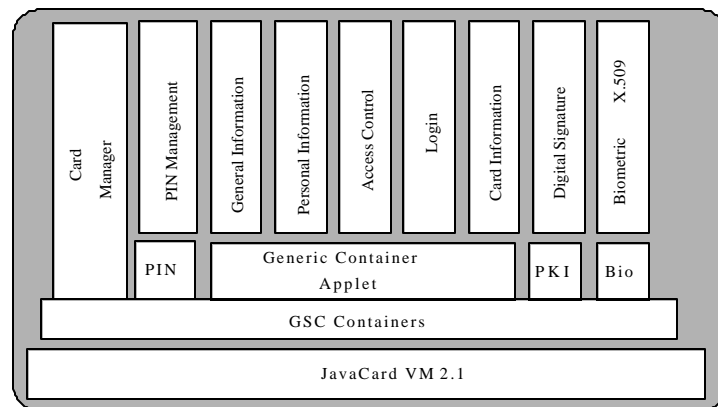
Contact-less

## Legacy Systems and Applications



Demographic Data  
Biometrics  
Clearance Data  
HR Training Qualifications and Other Data

Digital Photograph  
PKI Certificates  
Access Authorized





# ***TWIC System Performance Measurements***



## **TWIC System Performance Measurement Examples**

### **Impact on Security**

- Reduced intrusion attempts
- Security of biometric and personal data
- Local security plans supported
- Secure facilities using biometrics

### **Impact on Commerce**

- Reduced credential processing time
- Reduced stakeholder security investments
- Decrease in redundant credentials
- Reduced duplicative background checks
- Potential reduction in insurance costs
- Cost avoidance via leveraged investments

### **Customer / Stakeholder Satisfaction**

- Customer service surveys
- Informal feedback analysis
- Cardholder usage rates
- New application requests

### **Impact on Government Efficiency**

- Federal credentialing costs avoided
- State and local credentialing costs avoided
- Programs & projects integrated
- Employ economies of scale

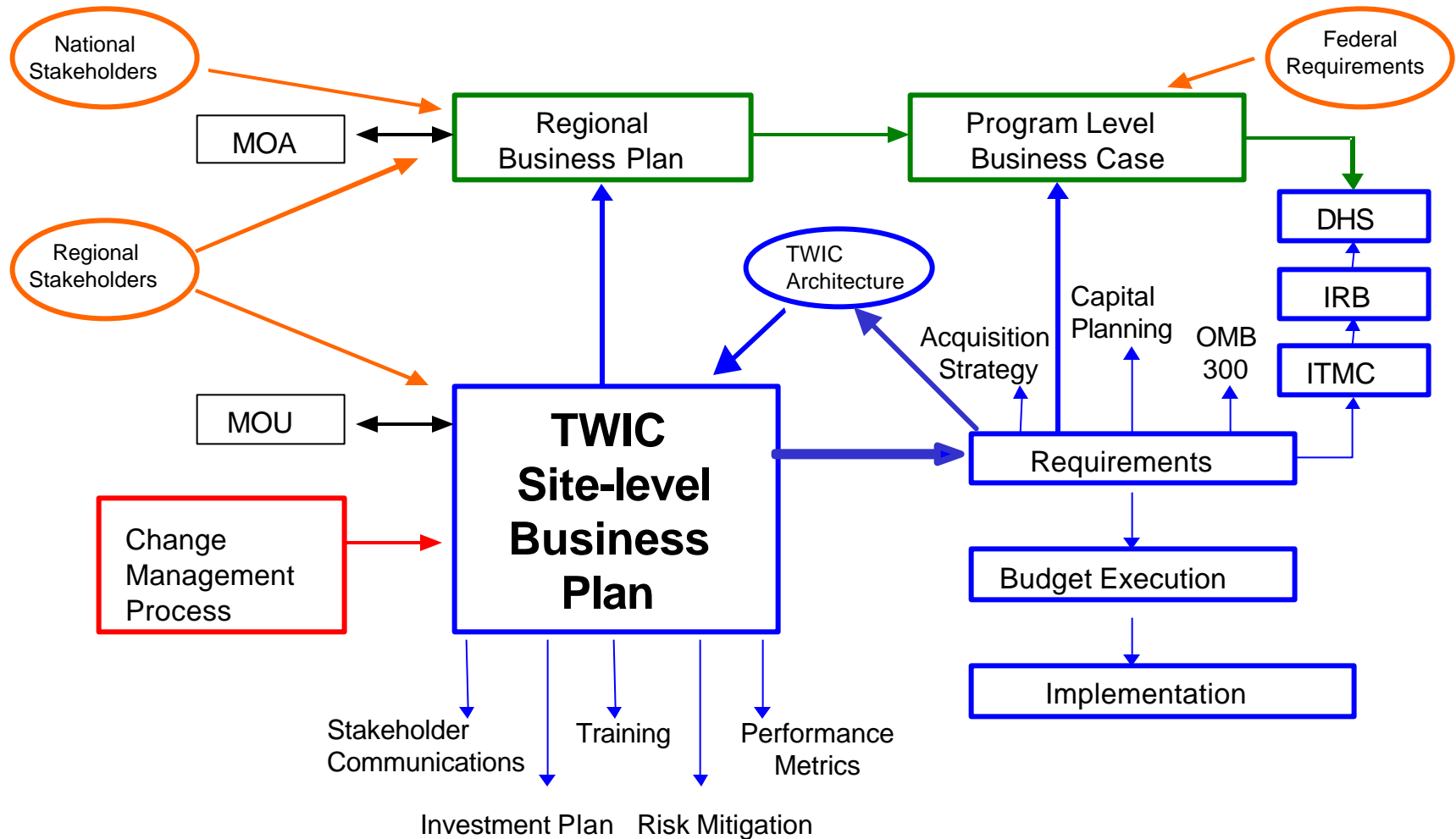
### **Technology Performance**

- IT systems reliability analysis
- Card failure rates
- Initial enrollment interventions
- Threat alerts across the system





# Business Based Methodology







## Working Group Resources



### Additional resources and expertise needed to address business policy issues

	Aviation Ops	Legal	Strategic Policy	OIT	Security	CTO	Revenue	M & L	Public Affairs
Topology	X	X	X	X		X			
Biometrics	X	X	X	X		X			
Trusted Agent	X	X	X	X	X				
Claimed ID	X	X	X	X	X				
Enrollment / Issuance	X	X	X	X	X	X	X		
Cost Sharing		X	X		X			X	
Background Checks	X	X	X	X	X				
Regulations		X	X						X
Privacy		X	X						X
Liability		X	X						X

Issues will be merged into 7 groups to balance resource workload:

- Topology / Biometrics
- Trusted Agent / Claimed ID / Enrollment
- Cost Sharing
- Background Checks
- Regulations
- Privacy
- Liability



## ***Conclusion***



## **TWIC Program Benefits**

### **Improves Security**

- Reduced risk of fraudulent or altered credentials
- Biometrics used for secure, positive match of individual to authorized access level and clearances
- Ability to interface and communicate with other federal, local, and state agencies
- Ability to disseminate “threat alerts” throughout a nationally integrated system

### **Protects Individual Privacy**

- Collection of minimum data elements
- Secure record control system and network
- Employs advanced information technology to protect personal information
- System-wide encryption implementation

### **Enhances Commerce**

- Increases process speed and efficiency
- Enables improved management and utilization of resources
- Expanded E-Gov potential
- Public – private partnership
- Economies of scale purchasing
- Eliminates need for redundant credentials and background investigations
- Potential to reduce industry insurance costs
- Leverages current security investment and legacy systems